Pragmio — WordPress Malware Cleanup

Evidence Report (Sample)

Generated: 2025-08-11 17:00 UTC
Client: example.com
Engineer: Pragmio Security Team
Case ID: PRG-WP-0001 (sample)

Summary

Active malware and backdoors were removed from the WordPress codebase and database. WordPress core, themes, and plugins were updated to the latest versions. Application hardening, key/salt rotation, and Cloudflare WAF rules were applied. Final scans show the site is clean. A 14-day same-vector warranty has been issued (sample report).

Actions Timeline

12:03 Site locked down; backups taken; maintenance mode enabled 12:12 Collected indicators of compromise; integrity scan completed 13:01 Removed infected files; restored clean copies from checksums 13:34 Database cleanup (removed injected payloads in wp_options/wp_posts) 14:05 Updated core, themes, and plugins to latest versions 14:28 Rotated salts/keys; audited users; removed weak accounts 14:50 Normalized file permissions (644/755); throttled XML-RPC 15:05 Applied Cloudflare WAF rules; set security headers 15:20 Final scan: CLEAN; warranty issued; evidence archived

Key Findings

- Backdoor loader in /wp-content/uploads/.cache/loader.php (removed) - Modified wp-config.php with eval() payload (cleaned; salts rotated) - Footer injection in theme functions.php (removed) - Database options contained base64_ and gzinflate payloads (cleaned)

Changed/Removed Files (excerpt)

```
/wp-includes/js/jquery/jquery.min.js     (replaced with official checksum)
/wp-content/uploads/.cache/loader.php    (removed backdoor)
/wp-content/themes/old-theme/functions.php (cleaned malicious footer injection)
/wp-config.php                            (cleaned; salts rotated)
```

Database Queries (excerpt)

```
SELECT option_id FROM wp_options WHERE option_value LIKE '%base64_%';
UPDATE wp_options SET option_value = REPLACE(option_value, '<payload>', '') WHERE option_id=...;
DELETE FROM wp_posts WHERE post_content LIKE '%gzinflate(%' AND post_type='revision';
```

Scans & External Checks

- Local integrity check: PASS
- Sucuri SiteCheck: CLEAN (screenshot archived)
- Google Search Console Security Issues: Review submitted

Warranty

14-day same-vector warranty (sample). “Same vector” = identical entry point exploited again (e.g., vulnerable plugin path). New vectors (installing a different vulnerable plugin, nulled themes, compromised admin device, server-level breach) are not covered.

Next Steps

- Remove abandoned 'old-theme'; delete unused plugins
- Enforce 2FA for admin users; use strong unique passwords
- Keep auto-updates on; verify offsite backups weekly
- Consider Maintenance plan (weekly updates, WAF tuning, priority response)